AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (Currently Amended) An advanced encryption standard (AES) engine with real time S-box generation comprising:

a Galois field multiplier system in a first mode responsive to a first data block for generating an AES selection (S-box) function by executing the multiplicative inverse ~~increase~~ in [[GF^{1}]] GF^{-1} (2^m) and applying an affine over GF(2) transformation to obtain a subbyte transformation; and

a shift register system for transforming said subbyte transformation to obtain a shift row transformation;

said Galois field multiplier system being responsive in a second mode to said shift row transformation to obtain a mix column transformation and adding a round key for generating in real time an advanced encryption standard cipher function of said first data block.

2. (Previously presented) The advanced encryption standard (AES) engine with real time S-box generation of claim 1 in which said first mode includes two states for executing m-1 cycles of operation including a first state for multiplying a subbyte by one to obtain a product and then squaring the product to obtain an intermediate result and repeating with the intermediate result m-2 times and a second state for performing the multiply and square operations one more time and transforming the final intermediate

result to obtain the subbyte transformation.

3. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 2 in which said Galois field multiplier system includes a Galois field linear transformer for each said mode.

4. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 2 in which said Galois field multiplier system includes a Galois field linear transformer for each state of said first mode and for said second mode.

5. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 2 in which said Galois field multiplier system includes a Galois field linear transformer and a program circuit for reconfiguring said Galois field linear transformer for each mode.

6. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 5 in which said program circuit further reconfigures said Galois field linear transformer for each state in said first mode.

7. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 5 in which said program circuit configures said Galois field linear transformer to perform a compound multiply-square operation in said first state.

8. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 5 in which said program circuit configures said Galois field linear transformer to perform a compound multiply-square operation in said first state and a compound multiply-square and affine subbyte transformation in said second state.

9. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 3 in which said Galois field linear transformer associated with said second mode is configured as a multiplier in said first state and as multiply-accumulate in said second state to perform a mix column transformation and add a round key for generating an advanced encryption standard cipher function of said first data block.

10. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 3 in which said Galois field linear transformer associated with said first state is configured as a multiplier to perform a compound multiply-square operation.

11. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 3 in which said Galois field linear transformer associated with said second state is configured as a multiply-adder to perform a compound multiply-square and affine subbyte transformation.

12. (Original) The advanced encryption standard (AES) engine with real time S-

box generation of claim 1 in which said Galois field multiplier system includes at least one Galois field linear transformer and an associated polynomial multiplier.

13. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 1 in which said Galois field multiplier system includes a reconfigurable matrix of cells.

14. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 1 further including a key generator for providing a plurality of round keys.

15. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 14 in which said key generator includes a key generator circuit responsive to a master key to generate said round keys.

16. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 15 in which said key generator circuit includes said Galois field multiplier system in a third mode for executing a multiplicative inverse in $GF^1(2^m)$ and applying affine over GF(2) transformation to obtain said round keys.

17. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 16 in which said round key includes a plurality of subkeys.

18. (Previously presented) The advanced encryption standard (AES) engine with real time S-box generation of claim 17 in which said third mode includes two states for executing m-1 cycles of operation including a third state for multiplying a subkey by one to obtain a product and then squaring the product to obtain an intermediate result and repeating with the intermediate result m-2 times and a fourth state for performing the multiply and square operations one more time and transforming the final infinite result to obtain the subkey transformation.

19. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 18 in which said Galois field multiplier system includes a Galois field transformer for each of said third and fourth states.

20. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 19 in which said Galois field linear transformer is reconfigured by said program circuit for said third mode.

21. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 20 in which said program circuit for further reconfigures said Galois field linear transformer for each of said third and fourth states in said third mode.

22. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 20 in which said program circuit configures said Galois field linear transformer to perform a compound multiply-square operation in said third state.

23. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 20 in which said program circuit configures said Galois field linear transformer to perform a compound multiply-square operation and affine subkey transformation in said fourth state.

24. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 18 in which said Galois field linear transformer associated with said third state mode is configured as a multiplier to perform a compound multiply-square operation.

25. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 18 in which said Galois field linear transformer associated with said fourth state is configured as a multiply-adder to perform a compound multiply-square and affine subkey transformation.

26. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 1 in which said Galois field multiplier system includes: a polynomial multiplier circuit for multiplying two polynomials with coefficients over a Galois field to obtain their product; a Galois field linear transformer responsive to said polynomial multiplier circuit for predicting the modulo remainder of the polynomial product for an irreducible polynomial; a storage circuit for supplying to said Galois field linear transformer a set of coefficients for predicting the modulo remainder for a predetermined irreducible polynomial; and a Galois field adder circuit for adding said product of said

multiplier circuit with a third polynomial with coefficients over a Galois field for performing the compound multiply and add operations in a single cycle.

27. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 1 in which said Galois field multiplier system includes: a polynomial multiplier circuit for multiplying two polynomials with coefficients over a Galois field to obtain their product; a Galois field linear transformer responsive to said polynomial multiplier circuit for predicting the modulo remainder of the polynomial product for an irreducible polynomial; a storage circuit for supplying to said Galois field linear transformer a set of coefficients for predicting the modulo remainder for a predetermined irreducible polynomial; and a Galois field adder circuit for adding said product of said multiplier circuit with an additive identity polynomial for performing a Galois field multiply function of the input polynomials in one cycle.

28. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 1 in which said Galois field multiplier system includes: a polynomial multiplier circuit for multiplying two polynomials with coefficients over a Galois field to obtain their product; a Galois field linear transformer responsive to said polynomial multiplier circuit for predicting the modulo remainder of the polynomial product for an irreducible polynomial; a storage circuit for supplying to said Galois field linear transformer a set of coefficients for predicting the modulo remainder for a predetermined irreducible polynomial; and a Galois field adder circuit for adding said product of said multiplier circuit with said output of said Galois field linear transformer circuit to obtain

Galois field multiply-accumulate function of the input polynomials in one cycle.

29. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 1 further including a plurality of Galois field multiplier systems for simultaneously processing a plurality of subbytes.

30. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 17 further including a plurality of Galois field multiplier systems for simultaneously processing a plurality of subkeys.

31. (Original) The advanced encryption standard (AES) engine with real time S-box generation of claim 3 in which said Galois field linear transformer has a matrix of cells for immediately predicting the modulo remainder of the succession of Galois field linear transforms of an irreducible Galois field polynominal to obtain the ultimate output of the Galois field linear transform directly in one transform cycle.